

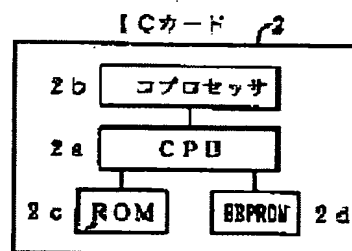
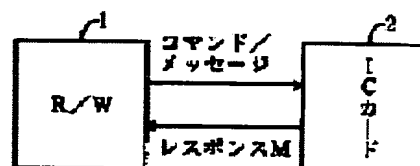
**IC CARD HAVING PROVISION AGAINST ATTACK TAKING ADVANTAGE OF FAILURE**

**Patent number:** JP11008616  
**Publication date:** 1999-01-12  
**Inventor:** HANDA FUKIO  
**Applicant:** DAINIPPON PRINTING CO LTD  
**Classification:**  
- **international:** H04L9/10; G06K19/073; G09C1/00; G09C1/00;  
H04L9/32  
- **european:**  
**Application number:** JP19970159992 19970617  
**Priority number(s):**

**Abstract of JP11008616**

**PROBLEM TO BE SOLVED:** To enhance the security against attack taking advantage of a failure of the IC card that conducts signature generating processing at a high speed by using the Chinese remainder theorem.

**SOLUTION:** The power remainder calculation generating a digital signature M is processed at a high speed with the Chinese remainder theorem by using a prime factor to modulus (n), and an error check code for data generated in the calculation process of the Chinese remainder theorem together with the data themselves are calculated and stored simultaneously. In the case of the digital signature M, the error check code of the data is again calculated, the stored error check code is collated to detect an error of the data and an error status is returned when the error is detected.



Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-8616

(43) 公開日 平成11年(1999) 1月12日

(51) Int.Cl.<sup>9</sup>

識別記号

F I

H 0 4 L 9/10

H 0 4 L 9/00

6 2 1 Z

G 0 6 K 19/073

G 0 9 C 1/00

6 5 0 Z

G 0 9 C 1/00

6 5 0

6 6 0 Z

6 6 0

6 6 0 A

G 0 6 K 19/00

P

審査請求 未請求 請求項の数 2 O L (全 7 頁) 最終頁に続く

(21) 出願番号

特願平9-159992

(22) 出願日

平成9年(1997) 6月17日

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 半田富己男

東京都新宿区市谷加賀町一丁目1番1号大

日本印刷株式会社内

(74) 代理人 弁理士 経川 昌信 (外7名)

(54) 【発明の名称】 故障利用攻撃対応 ICカード

(57) 【要約】

【課題】 中国人剰余定理を利用して高速に署名作成処理をするICカードの故障利用攻撃に対する安全性を高める。

【解決手段】 デジタル署名の作成を行う 冪乗剰余計算を法 $n$ の素因数を用いて中国人剰余定理により高速で処理し、中国人剰余定理による計算過程において生成されるデータとともに、該データについてのエラー検出符号を同時に計算して記憶しておき、デジタル署名の作成の際に、前記データのエラー検出符号を再度計算し、記憶しておいたエラー検出符号と照合してデータの誤りを検出し、誤りを検出した時にはエラーステータスを返すようにしたことを特徴とする。

	データ	CRCコード
(a)	$C_p$	X ( $C_p$ )
(b)	$C_a$	X ( $C_a$ )
(c)	$M_p$	X ( $M_p$ )
(d)	$M_a$	X ( $M_a$ )

$$\text{ステップ2: } M_p = C_p^x \bmod p, M_q = C_q^y \bmod q \quad \dots\dots(6)$$

ここに、 $x = d_p$ 、 $y = d_q$ を計算する。ステップ2での計算は、 $p$ 、 $q$  各々についての通常のRSA復号化計算

$$M \equiv M_p \pmod{p}$$

$$M \equiv M_q \pmod{q}$$

(7)式は $M - M_p$ が $p$ で割り切れ、(8)式は $M - M_q$ が $q$ で割り切れることを表している。

$$M = \{ a (M_p - M_q) \bmod p \} * q + M_q \quad \dots\dots(9)$$

の計算でデジタル署名 $M$ が求められる。

【0009】図7は上記した手順で高速でデジタル署名 $M$ を作成する処理フローを示している。ICカード2がデジタル署名のコマンドを受け取ると(実際にはコマンド名を受け取り、コマンド名に対応するコマンドをROMから読み出す)、ICカードではあらかじめEEPROMに記憶してある $d_p$ 、 $d_q$ 、 $a$ を読み出すとともに、コマンドとともに送られてくるメッセージを読み込む(ステップ1~2)。次いで、(5)式により $C \bmod p$ 、 $C \bmod q$ を計算して $C_p$ 、 $C_q$ を求め(ステップ3~4)、次いで、 $C_p$ 、 $C_q$ 、 $d_p$ 、 $d_q$ 、 $p$ 、 $q$ を用い、(6)式で $M_p$ 、 $M_q$ を計算する(ステップ5~6)。次いで、中国人剰余定理により(9)式を用いてデジタル署名 $M$ を作成し、作成したデジタル署名 $M$ をレスポンスとしてリーダー/ライター1へ返す。

【0010】このように、 $n$ に対して半分の桁数の $p$ 、

$$g \cdot c \cdot d((M')^* - C, n) \quad (g \cdot c \cdot d: \text{最大公約数}) \quad \dots\dots(10)$$

によって秘密に保つべき $n$ の素因数 $q$ が求められてしまう(Marc Joye and Jean-Jacques Quisquater, "Attacks on system using Chinese remaindering" November 1

$$M'^* \equiv C \pmod{n}$$

が成立するが、 $M_p'$ に誤りがあるため成立しない。そして

$$(M')^* \equiv C \pmod{q}$$

である。すなわち、 $(M')^* - C$ と $n (=pq)$ との最大公約数は $q$ である。こうして、 $q$ が分かると $p$ も分かり、その結果、すべての秘密情報が分かってしまうことになる。

【0013】

【発明が解決しようとする課題】このように、故障攻撃により秘密情報が解析されるため、中国人剰余定理を利用して計算したデジタル署名 $M$ が正しいか否かを確認する必要があるが、確認するには、作成されたデジタル署名を署名作成者自ら検証してみる必要があった。すなわち、署名作成者の公開鍵 $e$ を用いて $M'^* \equiv C \pmod{n}$ を検証する必要があった。

【0014】ところで、冪乗剰余計算を高速に処理するコプロセッサを搭載したICカードの場合、コプロセッサによる冪乗剰余計算の対象となる整数の大きさはハードウェア的に制限がある。前述したように、高速処理のためにデジタル署名の作成において冪乗剰余計算の法 $n$ の素因数 $p$ 、 $q$ を用いるので、 $p$ 、 $q$ の大きさをコプ

算である。この結果を用いると、(1)式は次の連立合同式に帰着する。

$$\dots\dots(7)$$

$$\dots\dots(8)$$

ステップ3: 中国人剰余定理より、

$q$ による剰余計算となるため、(1)式の計算に比して計算量がほぼ $1/4$ となり、処理を高速化できる。

【0011】ところで故障利用攻撃では、デジタル署名を作成するICカードに対して、外部から物理的刺激(熱、圧力、放射線、電圧等)を加えることにより、ICカードのメモリやレジスタ上のビットパターンの一部に故意に誤りを発生させる。例えば、前記ステップ2の(6)式の計算途中で、故意に誤りを発生させ、 $M_p$ または $M_q$ のどちらか一方の値を誤らせる。ここでは、 $M_p$ の計算結果が誤っているとしてそれを $M_p'$ とし、 $M_q$ は正しく求められているとする。 $M_p'$ 、 $M_q$ を(9)式に適用して求めた署名 $M$ も誤っていることになるから、それを $M'$ とする。

【0012】このとき、署名対象データ $C$ と公開されている法 $n$ の値を使って、

1,1996 この論文は<http://www.dice.ucl.ac.be/crypto/techreports.html>にて公開されている。なぜならば、 $M$ が正しいとすると

$$\dots\dots(11)$$

$$M_p' \equiv C_p^x \pmod{p} \quad (x = d_p)$$

なので、

$$\dots\dots(12)$$

ロセッサで扱える限度いっぱいまでとると、 $p$ 、 $q$ の積である $n$ はコプロセッサで扱える限度を超えてしまう。署名の検証は $e$ 、 $n$ のみ用いて $M'^* \equiv C \pmod{n}$ をコプロセッサで演算して行うが、この演算を行うことができなくなってしまう。一方、CPUの命令を用いてソフトウェアでの処理により検証すると、署名の作成本体処理よりもはるかに多くの時間を要するため、故障利用攻撃を受けたかどうかの検証を実用的なレスポンス時間内に行うことができない。そのため、 $n$ の大きさがコプロセッサで扱える限度を超える場合には、作成した署名の検証を行わないことが一般的であり、故障利用攻撃を許してしまう結果となっていた。

【0015】本発明は上記課題を解決するためのもので、メッセージ作成者本人がRSA秘密鍵を用いてデジタル署名を作成する際に、中国人剰余定理を利用して高速に署名作成処理をするICカードに対して、中国人剰余定理の途中結果に計算誤りを発生させ、誤ったデジタル署名を作らせることによって、秘密情報を得よう

デジタル署名作成処理フローを説明する。ICカードがデジタル署名のコマンドを受け取ると、ICカードではあらかじめEEPROMに記憶してある $d_p$ 、 $d_a$ 、 $a$ を読み出すとともに、コマンドとともに送られてくるメッセージを読み込む(ステップ11~12)。次いで、(5)式により $C \bmod p$ を計算して $C_p$ を求めるとともに、 $C_p$ のCRCコード $X(C_p)$ を計算して記憶する(ステップ13)。同様に、 $C \bmod q$ を計算して $C_q$ を求めるとともに、 $C_q$ のCRCコード $X(C_q)$ を計算して記憶する(ステップ14)。また、(6)式で $M_p$ 、 $M_q$ を計算するとともに、 $M_p$ 、 $M_q$ のCRCコード $X(M_p)$ 、 $X(M_q)$ を計算してそれぞれ記憶する(ステップ15、16)。次いで、デジタル署名を作成する段階で、再び $C_p$ 、 $C_q$ 、 $M_p$ 、 $M_q$ のCRCコードを計算し、記憶しておいたCRCコード $X(C_p)$ 、 $X(C_q)$ 、 $X(M_p)$ 、 $X(M_q)$ とそれぞれ照合する(ステップ17~20)。

【0024】この照合は、図4に示すように、記憶しておいたCRCコード $X(Y)$ と、計算した $Y$ のCRCコード $T$ とを比較し、両者が一致すれば正常終了、一致しなければ異常終了とする。図3のステップ17~20のどの段階で異常終了となっても、その時点でエラーのステータスワードをリーダー/ライターに返して処理を終了する。ステップ17~20がすべて正常終了の場合、デジタル署名を作成して、これをレスポンスとして返す(ステップ21、22)。

【0025】

【発明の効果】以上のように本発明によれば、 $n$ の大きさがコプロセッサで扱える限度を超える場合にも、作成した署名の検証を短時間で行うことができるので、故障利用攻撃を受けても、誤ったデジタル署名をレスポンスとして返してしまう可能性を減らすことができる。故障利用攻撃によって、エラー検出符号そのものに誤りが発生したり、エラー検出符号の誤り検出能力を超える範囲の誤りが発生する可能性が全くないとはいえないが、ほとんどの場合において故障利用攻撃を受けたことを検出することが可能である。

【図面の簡単な説明】

【図1】 エラー検出符号としてCRCコードを用いた例を説明する図である。

【図2】 エラー検出符号としてパリティチェックを用いた例を説明する図である。

【図3】 本発明のデジタル署名作成処理フローを説明する図である。

【図4】 CRC照合処理を説明する図である。

【図5】 リーダー/ライターとICカードとの通信を説明する図である。

【図6】 ICカードの説明図である。

【図7】 従来のデジタル署名作成処理フローの説明図である。

【符号の説明】

1…リーダー/ライター、2…ICカード、2a…CPU、2b…コプロセッサ、2c…ROM、2d…EEPROM、 $M_a$ 。

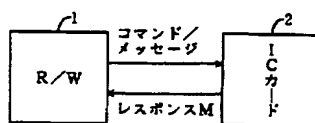
【図1】

	データ	CRCコード
(a)	$C_p$	$X(C_p)$
(b)	$C_q$	$X(C_q)$
(c)	$M_p$	$X(M_p)$
(d)	$M_q$	$X(M_q)$

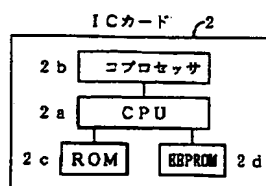
【図2】

	データ	パリティビット
(a)	$C_p$	$P(C_p)$
(b)	$C_q$	$P(C_q)$
(c)	$M_p$	$P(M_p)$
(d)	$M_q$	$P(M_q)$

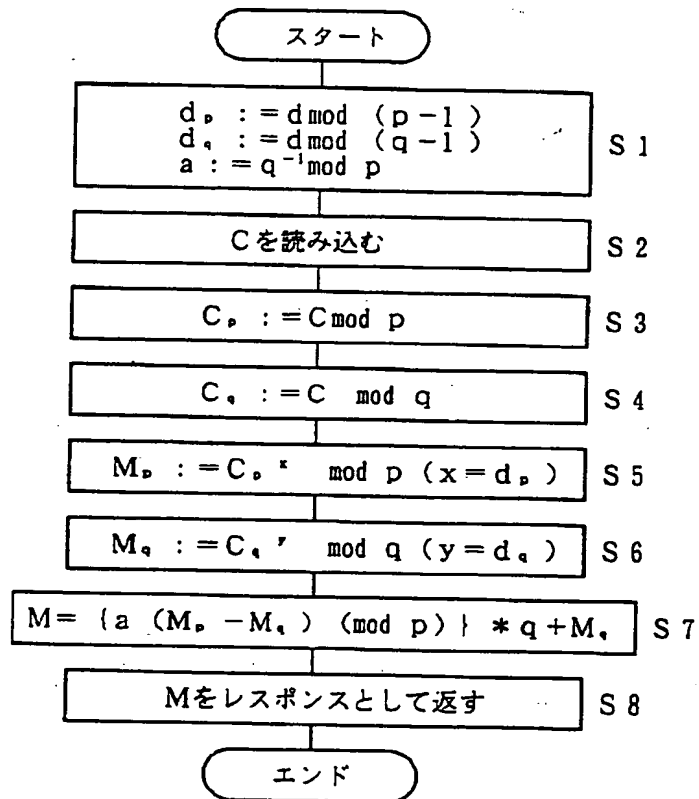
【図5】



【図6】



【図7】



フロントページの続き

(51)IntCl.<sup>a</sup>

識別記号

FI

H04L 9/32

H04L 9/00

673E